United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FRANK D. RUSSO, ET AL., Plaintiffs**,** vs. **MICROSOFT CORPORATION,** Defendant**.**	CASE NO. 4:20-cv-04818-YGR **ORDER GRANTING DEFENDANT MICROSOFT CORPORATION'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT** Re: Dkt. No. 25

Plaintiffs Frank D. Russo; Koonan Litigation Consulting, LLC; and Sumner M. Davenport & Associates, LLC (collectively, "Plaintiffs") bring this class action against Defendant Microsoft Corporation for violation of privacy laws. (Dkt. No. 29 ("Comp.").) Plaintiffs allege violations of (1) the Wiretap Act, 18 U.S.C. § 2511, *et seq.*, (2) the Stored Communications Act ("SCA"), 18 U.S. C. § 2701 *et seq.*, (3) the Washington Consumer Protection Act ("WCPA"), Wash. Rev. Code 9,73.010 *et seq.*, (4) Washington Privacy Act ("WPA"), Wash. Rev. Code 9.73.010 *et seq.*, and (5) intrusion upon seclusion under Washington law.

Now before the Court is Microsoft's motion to dismiss. (Dkt. No. 25 ("Mot.").) Having considered the papers submitted and the pleadings in this action, and for the reasons below, the Court hereby **GRANTS IN PART** and **DENIES IN PART** the motion to dismiss.[1]

I. BACKGROUND

Plaintiffs use Microsoft's software to conduct business. Mr. Russo uses Microsoft 365 Business Standard for his sole proprietorship, Russo Meditation & Law, to provide mediation, arbitration, and alternative dispute resolution services to clients. (Comp. ¶¶ 13-15.) Koonan Litigation Consulting, LLC employs Microsoft 356 Business Basic to provide advice on "all

[1] The Court finds the motion appropriate for resolution without oral argument and the matter is deemed submitted. Fed. R. Civ. P. 78(b); Civ. L. R. 7-1(b).

aspects of litigation." (*Id.* ¶¶ 20-23.) Sumner M. Davenport & Associates, LLC similarly uses Microsoft 365 Business Basic to provide marketing services. (*Id.* ¶¶ 28-34.) Each product provides cloud-based access to Microsoft's Office software suite for a monthly subscription fee. (*Id.* ¶ 46.)

Plaintiffs allege that Microsoft (1) shared its business customers' data with Facebook, (2) shared its business customers data with third-party developers, (3) shared its business customers' data with subcontractors to support Microsoft's products, and (4) used business customers' data to develop and sell new products and services through their software without consent. (*Id.* ¶ 1.)

Although the precise nature of plaintiffs' claims lacks clarity, the complaint appears to quote from various documents related to different features.[2] First, with respect to Facebook data sharing, plaintiffs quote from a technical document describing "Facebook Contact Sync," which "shares information in your Outlook Contacts folder with Facebook and imports your Facebook friends' contact information into your Outlook Contacts folder." (*Id.* ¶ 76; Dkt. No. 25-1 at 12.) Although the complaint acknowledges that this feature can be disabled, it states that "the damage has already been done" at that point because "[o]nce contacts are transferred to Facebook, they cannot be deleted from Facebook's system except by Facebook." (Comp. ¶ 76.)

Second, with respect to third-party developers, plaintiffs apparently refer to "Microsoft Graph," which allows developers to "build smarter apps" for Windows using APIs that "model and represent people in Microsoft 365 services," including by "perform[ing] searches for people who are relevant to the signed-in user and have expressed an interest in communicating with that user over certain 'topics.'" (*Id.* ¶ 84; Dkt. No. 25-1 at 51, 53.) Although plaintiffs apparently acknowledge that this feature requires user permission, they allege that "Microsoft nonetheless transmits [a] non-consenting business customer's data to third-party developers if *another* Office 365 user consented to the application." (Comp. ¶ 82 (emphasis in original); *see* Dkt. No. 25-1 at

[2] The Court **GRANTS** Microsoft's request for judicial notice of these documents. (Dkt. No. 25-2.) The statements in these documents form the basis of Plaintiffs' claims and are therefore incorporated by reference. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1022 (9th Cir 2018). Plaintiffs do not oppose Microsoft's request, but, on the contrary, also quote from those documents to support their claims. (*See, e.g.*, Dkt No. 29 ("Oppo.") at 3.)

53.) For instance, if a signed-in user give consent, the API allows a developer to search that user's email to find other users who have communicated about particular topics. (*See id.*)

Third, with respect to subcontractors, plaintiffs allege generally that Microsoft uses subcontractors "not only to provide customers with the services they purchased, but also to serve Microsoft's separate commercial ventures, including discovering new business insights and developing new services, products, or features," without requiring anonymization or encryption. (Comp. ¶¶ 87-90.) The factual basis for this claim is not alleged.

Finally, with respect to using data to develop new products, plaintiffs refer to the following products: Security Graph API, Microsoft Audience Network, Windows Defender Application Control, Azure Advanced Threat Protection, Advanced Threat Protection, and Cortana. (*Id.* ¶¶ 93-97.) Plaintiffs allege facts for only the first two products and Cortana. Security Graph is an API provided to developers "so they can create new security-related products" that is allegedly built by "scanning '400 billion' . . . customers' emails and 'data from 700 million Azure user accounts.'" (*Id.* ¶¶ 93-94.) Microsoft Audience Network appears to be an advertisement product that imparts "rich user understanding" through "robust data sets." (*Id.* ¶ 95.) Cortana allegedly "collects and uses business customer data (including documents, contacts, and calendar information)" to "develop and improve" its service. (*Id.* ¶ 97.)

Plaintiffs claim that Microsoft's practices are contrary to its marketing representations and contracts, which tout its privacy protections. (*Id.* § B.) For instance, Microsoft's "Trust Center" website allegedly states that "[w]e use your data for just what you pay us for: to maintain and provide Office 365" and "only to provide the services." (*Id.* ¶ 58.) Its Online Service Terms similarly allegedly state that it will use customer data only to "[d]eliver[] functional capabilities," "troubleshoot[] problems," and "improv[e] the product through updates." (*Id.* ¶ 65.) Indeed, the terms allegedly promise that customer data will not be used for "(a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions." (*Id.* ¶ 66.) Plaintiffs claim that they would not have purchased Microsoft's products if they knew the truth about their use. (*Id.* ¶ 114.)

II. Legal Standard

Under Federal Rule of Civil Procedure 12(b)(6), a complaint may be dismissed for failure to state a claim upon which relief may be granted. Dismissal for failure under Rule 12(b)(6) is proper if there is a "lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Conservation Force v. Salazar*, 646 F.3d 1240, 1242 (9th Cir. 2011) (quoting *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1988)). The complaint must plead "enough facts to state a claim [for] relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is plausible on its face "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. If the facts alleged do not support a reasonable inference of liability, stronger than a mere possibility, the claim must be dismissed. *Id*. at 678-79; *see also In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (stating that a court is not required to accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences").

If a court dismisses a complaint, it should give leave to amend unless "the pleading could not possibly be cured by the allegation of other facts." *Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv. Inc.*, 911 F.2d 242, 247 (9th Cir. 1990).

III. Analysis

A. Plaintiffs Have Not Shown Standing.

To bring a claim in federal court, a plaintiff needs to have standing. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559-60 (1992). Article III standing requires plaintiffs to have "(1) suffered injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, -- U.S. --, 136 S. Ct. 1540, 1547 (2016). Plaintiffs who have not been personally injured in by defendant's conduct lack a "personal stake" in the outcome and thus have no standing. *Id*. at 1548; *see also Raines v. Byrd*, 521 U.S. 811, 818-19 (1997). The party invoking federal jurisdiction must "clearly allege facts demonstrating each element" of standing at the motion to dismiss stage. *Spokeo*, 136 S.Ct at 1547 (simplified).

Here, plaintiffs do not allege enough facts to draw a reasonable inference that they have been injured by Microsoft's conduct. With respect to Facebook Connect, plaintiffs do not allege that they have used Outlook, much less that they added anyone to their Outlook Contacts folder who could have been disclosed to Facebook. With respect to third-party developers, plaintiffs do not allege any user with whom they communicated that granted consent for Microsoft Graph to scan their emails. With respect to both subcontractors and Microsoft's other products, plaintiffs do not allege any facts that could support a reasonable inference that Microsoft's cloud software customers were affected at all. For instance, plaintiffs do not explain how the information for Advanced Threat Protection was gathered and how involved Office 365 customers.

Instead, plaintiffs cite two paragraphs that generically state that Microsoft used and shared "Plaintiffs' and Class Members'" data, including their emails, as described above. (*See* Comp. ¶¶ 141, 143.) Such allegations are far too sparse and conclusory to make the claim of personal injury plausible. *See Gilead*, 536 F.3d at 1055; *cf. In re Chrysler-Dodge-Jeep Ecodiesel Mktg., Sales Practices, & Product Liability Litig.*, 295 F. Supp. 3d 927, 949 (N.D. Cal. 2018) (no standing based on overpayment theory where plaintiffs do not allege that *their* products were defective). The Court thus dismisses the complaint for failure to allege facts demonstrating standing.[3]

B. Plaintiffs Have Not Stated a Claim.

For similar and additional reasons, plaintiffs have failed to state a claim on the merits. As an initial matter, plaintiffs' allegations concerning subcontractors and use of customer data to develop new products (the third and fourth set of alleged conduct) are too conclusory to render their claims plausible. Based on plaintiffs' complaint, Microsoft *could* be using customer data and

[3] In addition to Article III, the statutes here limit the types of injuries sufficient for a party to bring suit. The Wiretap Act provides a cause of action only to persons "whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used." 18 U.S.C. § 2520. The SCA provides a cause of action to a person "aggrieved by any violation," 18 U.S.C. § 2707(a), which typically requires a plaintiff to "allege[] with particularity that *her* communications were part of the [disclosure]." *Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 910 (9th Cir. 2011) (emphasis in original). Further, the WPA provides a cause of action only to those "claiming that a violation of this statute has injured his or her business, his or her person, or his or her reputation." Wash. Rev. Code § 9.73.060. Thus, because plaintiffs fail to allege Article III standing, they also fail to state a claim under these statutes.

subcontractors to develop new products. That said, plaintiffs allege no facts to suggest that this *actually* happens. Similarly, plaintiffs do not allege that Microsoft Audience Network actually involves Office 365 products. The complaint thus fails to allege enough facts to nudge claims from "mere possibility" to plausibility. *Iqbal*, 556 U.S. at 678. Thus, the Court evaluates only the alleged features for which Plaintiffs provide sufficient factual allegations, namely: (1) Facebook Connect, (2) Microsoft Graph API, (3) Security Graph API, and (4) Cortana. *See supra* § I.

1. *Court One: Wiretap Act*

The Wiretap Act provides relief against any person who "intentionally intercepts . . . the contents of any electronic communication," or who "intentionally discloses" or "intentionally uses" such content while "knowing or having reason to know" it was so intercepted. 18 U.S.C. §§ 2511(1)(a), (c)-(d). Microsoft moves to dismiss on three grounds: (1) the alleged conduct does not involve "contents" of communications, (2) any communications would have been stored prior to access and therefore not "intercepted" while in transmission, and (3) the "ordinary course of business" exception applies.

With respect to communication contents, plaintiffs sufficiently allege that Graph and Security Graph are developed or improved by scanning email. (Comp. ¶¶ 84, 94-95.) Thus, to the extent that plaintiffs can allege that *their* emails were scanned, they will have stated a claim under the Wiretap Act.[4] *See Doe v. Chao*, 540 U.S. 614, 624-25 (2004) (explaining that standing and the existence of cause of action involve separate inquiries). However, the Court agrees that Facebook Connect, which involves contact lists, cannot form the basis of a Wiretap Act claim. *See In re Zynga Privacy Litig.*, 750 F.3d 1098 (9th Cir. 2014) (name and identity data does not represent "contents"). Nor can Cortana, which allegedly scans "documents, contacts, and calendar information," not communications. (Comp. ¶ 97.)

With respect to interception, the complaint does not allege enough facts to determine whether the Graph and Security Graph scan stored or transmitted content. Ordinarily, this would

[4] Judicially noticed documents suggest that not all of the subscription products purchased by plaintiffs include Outlook, which raises serious doubts about their ability to state a claim based on email scanning for those products.

render plaintiffs' claims insufficient. In this case, however, plaintiffs plausibly argue that they do not know the precise nature of Microsoft's email scanning, as the information resides with the defendant, and plead the Wiretap Act and SCA claims in the alternative. The Court will permit plaintiffs to plead in the alternative because the point of scanning is not generally known. *See In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1027-28 (N.D. Cal. 2014). Namely, the Ninth Circuit has permitted "interception" claims where information was either "captured or redirected" during transit. *Noel v. Hall*, 568 F.3d 743, 751 (9th Cir. 2009). The Court finds plausible plaintiffs' allegations of scanning, since they are based on Microsoft's documents, and concludes that the precise point of scanning is an issue best left for summary judgment. *See Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 840-41 (N.D. Cal. 2014).

With respect to the ordinary course of business exception,[5] the rule applies only to conduct that "facilitates the transmission of the communication at issue or is incidental to the transmission of such communication." *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 818 (N.D. Cal. 2020) (citation omitted). In other words, there must be "some nexus" between interception and the provision of the service at issue. *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *11 (N.D. Cal. Sept. 26, 2013). The precise closeness of the required nexus remains unsettled, but courts broadly agree that "not everything [a party] does in the course of its business would fall within the exception." *Matera v. Google Inc.*, 2016 WL 8200619, at **7-9 (N.D. Cal. Aug. 12, 2016); *see, e.g.*, *Campbell*, 77. F. Supp. 3d at 844 (advertising is not part of the "ordinary business" of providing social networking services).

Here, Microsoft claims that the challenged conduct relates to features of Office 365, which are necessarily "incident" to provision of that service. With respect Cortana and Advanced Threat Protection, the Court agrees. Plaintiffs expressly allege that Cortana was part of their Office 365 subscription, and judicially noticed documents show the same for Advanced Threat Protection. (Comp. ¶ 97; Dkt. No. 25-1 at 63.) Even if plaintiffs did not personally use these features, they

[5] The "ordinary business exception" arises from a phrase in the statute: the Wiretap Act defines interception as requiring a "device" and then defines "device" to exclude those "used by a provider of wire or electronic communication service in the ordinary course of business." *See* 18 U.S.C. §§2510(4), 2510(5)(a)(ii).

specifically purchased them and cannot now complaint that Microsoft collects data necessary to provide them. With respect to Graph and Security Graph APIs, however, plaintiffs allege that Microsoft sells these APIs to developers, not to customers. (*Id.* ¶¶ 81, 93.) Drawing all inferences in favor of plaintiffs, data interception to develop the graph APIs are not "incident" to provision of service to *plaintiffs*.

Accordingly, to the extent that plaintiffs can allege that their specific emails were scanned, the complaint may state a claim under the Wiretap Act based on the Graph and Security Graph API features. The claims based on other features are dismissed with prejudice.

2. *Count Two: Stored Communications Act*

The SCA imposes liability on "electronic communication service" providers who "knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). It also imposes liability on "remote computer service" providers who do the same for communication contents "carried or maintained on that service" "(A) on behalf of, and received by means of electronic transmission from . . . a subscriber or customer of such service," or "(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." 18 U.S.C. § 2702(a)(2).

Microsoft moves to dismiss because (1) the allegations do not involve "contents" of communications, (2) the "necessarily incident" exception applies, and (3) the statute does not apply to Microsoft's own use of data. The Court has already found that plaintiffs sufficiently allege that Microsoft intercepted the contents of communications for Graph and Security Graph APIs (but not other features). Moreover, the Court has already found that the scanning was not part of Microsoft's ordinary course of business. While the "necessarily incident" exception under the SCA may, conceivably, have different scope, Microsoft cites no authority to show that is the case, and the argument fails for the same reasons.[6] Last, plaintiffs plausibly allege that Graph and

[6] The SCA exempts from liability divulging data "as may be necessarily incident to the rendition of the [defendant's] service." 18 U.S.C. § 2702(c)(3).

Security Graph APIs involve disclosures to third-party developers, which goes beyond Microsoft's own use of data. (Comp. ¶¶ 82, 93.) That is sufficient to state a claim for those features only.

Accordingly, to the extent that plaintiffs can allege that their specific emails were scanned, the complaint may state a claim based on Graph and Security Graph APIs. The claims based on other features are dismissed with prejudice.

3. *Count Three: Washington Consumer Protection Act*

To state a claim under the WCPA, plaintiffs must allege facts establishing "(1) an unfair or deceptive act or practice that (2) affects trade or commerce and (3) impacts the public interest, and (4) the plaintiff sustained damage to business or property that was (5) caused by the unfair or deceptive act or practice." *Keodalah v. Allstate Ins. Co.*, 194 Wash. 2d 339, 349-50 (2019). Microsoft challenges plaintiffs' compliance with the fourth and fifth elements—injury and causation—and further argues that the complaint fails to comply with the heightened pleading standard required for pleading fraud under Rule 9(b).

Starting with the first issue, plaintiffs claim an overpayment theory of injury where they "paid more for a service or product advertised as having certain qualities . . . when in fact the product did not have those qualities." (Comp. ¶ 167.) That states a cognizable injury under the WCPA, and plaintiffs plead enough factual content to make it plausible. Namely, plaintiffs allege that Microsoft publicly recognizes that its success "depends on [the] ability to win and retain [its] users' trust" and identifies privacy as a "competitive differentiator." (*Id.* ¶¶ 48-49.) The Court finds it plausible that, if Microsoft lacked its "competitive differentiator," it may have charged less for the subscriptions.[7] This also satisfies causation under a theory that plaintiffs overpaid for their subscriptions regardless of whether they were exposed to the misrepresentations. *See Kelley v. Microsoft Corp.*, 251 F.R.D. 544, 557-59 (W.D. Wash. 2008) (permitting class certification under price inflation theory). *But see Kelley v. Microsoft Corp.*, No. C07-0475 MJP, 2009 WL 413509,

[7] Plaintiffs also allege that they "would not have purchased [their] subscription, or alternatively would have paid less for it," if they knew the truth. (*E.g.*, Comp. ¶ 26.) However, because they do not allege that they saw any misrepresentation (but merely "believed" that their data would be secure), this theory fails to satisfy causation. *Cf. McGee v. S-L Snacks Nat'l*, 982 F.3d 700, 706 (9th Cir. 2020) (no standing under "benefit of the bargain" theory based on mere assumptions or beliefs).

at *6 (W.D. Wash. Feb. 18, 2009) (decertifying the class where plaintiffs failed to link specific customer demand to the misrepresentation).

However, the Court agrees that the complaint utterly fails the requirements of Rule 9(b). Rule 9(b) applies "where a claim is based on 'a unified course of fraudulent conduct,' even if the word 'fraud' is not used." *Water & Sanitation Health, Inc. v. Rainforest All., Inc.*, C15-75RAJ, 2015 WL 12657110, at *5 (W.D. Wash. Dec. 29, 2015) (citation omitted). It also applies "where fraud is an essential element of a claim or where Plaintiffs allege some fraudulent and some non-fraudulent conduct." *Id*. (citation omitted). Here, the complaint plainly alleges a "unified course of fraudulent conduct." *Id.* Plaintiffs claim that Microsoft "misleads its business customers as to how it shares and uses their data," "misrepresented and did not disclose" material facts that were directly contrary to its representations, and duped customers into sharing data it knew to be highly sensitive to obtain a commercial benefit. (*See* Comp. ¶¶ 100, 37, 50, 81.) These are exactly the type of circumstances where Rule 9(b) must apply to protect defendants' reputation from spurious (but highly damaging) allegations of fraud.[8] *See Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1104 (9th Cir. 2003).

Plaintiffs fail to meet that standard. Although the allegations are barely sufficient to meet the requirements for a "short and plain statement" under Rule 8 (mostly because they quote from Microsoft's own documents), they leave the public entirely in the dark about the nature of the purported data misuse. Microsoft apparently had to sort through—and then request judicial notice for—obscure technical documentation just to identify features that plaintiffs are accusing. The Court still has no idea how those features function, which parties use them, the form in which the data is provided, or anything else about them.[9] In short, plaintiffs do not plead nearly enough facts

[8] Plaintiffs implausibly argue that the CPA claim is based on mere "capacity to deceive the purchasing public." (Comp. ¶ 164.) That makes little sense. The complaint states that Microsoft knowingly makes privacy a central tenet of its marketing campaign and then knowingly takes a course of action directly contrary to it. (*Id.* ¶¶ 3, 81.) The mere absence of the words "intent to deceive" does not defeat Rule 9(b) where fraud is the clear implication of the allegations.

[9] These deficiencies are far from technical. Microsoft claims, for instance, that some of the accused features are provided to network administrators to protect their organizational networks—an entirely different privacy context than plaintiffs' allegations suggest that significantly impacts the plausibility of plaintiffs' claims.

to justify the gravity of their claims.

Accordingly, the Court dismisses the Washington CPA claim without prejudice.

4. *Count Four: Washington Privacy Act*

The WPA prohibits interception and recording of a "[p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state . . . without first obtaining consent of all the participants in the communication." Wash. Rev. Code § 9.73.010(1)(a). Microsoft moves to dismiss because (1) plaintiffs do not allege interception of private communications, (2) the WPA does not apply to corporations, and (3) the WPA does not apply extraterritorially.

As explained above, the Court agrees that plaintiffs have not alleged that their own communications were intercepted (private or otherwise). They therefore have no standing to bring a WPA claim.[10] Microsoft's other arguments lack merit.

Although the WPA does not define "person," it uses the term consistent with a broad definition that includes corporations. For instance, it imposes liability on conduct by "any individual, partnership, corporation, association, or the State of Washington, its agencies, and political subdivisions," but then provides a cause of action against any "person" who violates the statute. *See* Wash. Rev. Code §§ 9.73.010(1)(a), 9.73.060. Under Microsoft's interpretation, the Washington Legislature created liability against a broad range of entities, but only provided a cause of action against individuals, which is implausible. Similarly, the WPA defines common carriers as including "any person engaged as a . . . public service *company*" in certain fields, which demonstrates that companies are persons. Wash. Rev. Code § 9.73.070. Microsoft's argument to the contrary focuses on the use of the words "his or her" in section 9.73.060, but Microsoft does not contend that the other use of "person" in that section excludes corporations. *See* Wash. Rev. Code § 9.73.060 (using "person" to refer to both the party violating the statute and the party that can bring a claim). Because the Washington Legislature presumably used the term "person"

[10] Plaintiffs again claim an economic injury because "would not have purchased (or would have paid less for" services absent misrepresentations. That claim again fails because plaintiffs do not allege that their own services were affected by the alleged conduct.

consistently in that subsection, Microsoft's argument fails to persuade.

As for extraterritoriality, "the test for whether a recording of a conversation or communication is lawful is determined under the laws of the place of the recording." *State v. Fowler*, 157 Wash. 2d 387, 395 (2006) (en banc). The WPA "does not limit the territory in which telephone calls may be intercepted, as long as the interception occurs in Washington. *Kadoranian by Peach v. Bellingham Police Dept.*, 119 Wash. 2d 178, 184 (1992) (en banc); *see also* Wash. Rev. Code § 9.73.010(1)(a) (protecting communications "between points within or without the state"). As explained above, the Court finds that the precise points of interception is an issue best tested through discovery and does not dismiss on this ground, notwithstanding allegations that plaintiffs' communications originated in California and Wyoming.[11]

Accordingly, to the extent that plaintiffs can allege that their private communications were intercepted, they may state a claim under the WPA based on Graph and Security Graph APIs.

5. *Count Five: Intrusion Upon Seclusion*

Under Washington law, invasion of privacy through intrusion "consists of a deliberate intrusion, physical or otherwise, into a person's solitude, seclusion, or private affairs." *Fisher v. State ex rel. Dept. of Health*, 125 Wash. App. 869, 879 (2005); *see also Eastwood v. Cascade Broadcasting Co.*, 106 Wash. 2d 466 (1986) (intrusion upon seclusion is a sub-type of invasion of privacy under Washington law). Microsoft moves to dismiss the claim because (1) businesses do not have privacy rights, (2) plaintiffs voluntarily provided their information, and (3) the intrusion at issue is not "highly offensive."

The Court agrees with the first argument and dismisses on that ground. "[A] corporation has no personal right of privacy and thus has no cause of action for invasion of privacy." *Life Designs Ranch, Inc. v. Sommer*, 191 Wash. App. 320, 338 (2015); *see* Restatement (Second) of Torts § 652I, comment c (1976). Plaintiffs do not dispute this common sensical proposition, but

[11] Plaintiffs rely on the statement that "[o]f course, [WPA] may be violated by a recording made outside of this state if the recording was made for use of the evidence in Washington by an agent of a Washington official or other person." *Fowler*, 157 Wash. 2d at 347. The import of this statement—which appears to contradict the test articulated in the opinion—is not clear. The Court interprets it narrowly to apply to recordings by state officials for use in criminal proceedings.

argue that Mr. Russo, as an individual, may bring an intrusion upon seclusion claim. However, Mr. Russo never alleges that he used Microsoft's products for his *own* "private affairs." Instead, the complaint states that Mr. Russo used his subscription "in the course of his business," which consists of "mediation, arbitration, and alternative dispute resolution services." (Comp. ¶¶ 13, 15.) At most, the complaint suggests that Mr. Russo may have used the products for his clients' private affairs. Plaintiffs cite no case to suggest that Mr. Russo has standing to bring other people's common law tort claims, and the claim is improper.

Accordingly, the Court dismisses Mr. Russo's intrusion upon seclusion claim without prejudice and the other plaintiffs' claims with prejudice.

IV. CONCLUSION

For the foregoing reasons, the Court **GRANTS** Microsoft's motion to dismiss. The dismissal is without prejudice unless stated otherwise. Plaintiffs may file an amended complaint within twenty-one days.

IT IS SO ORDERED.

Dated: June 30, 2021

YVONNE GONZALEZ ROGERS
UNITED STATES DISTRICT COURT JUDGE

United States District Court
Northern District of California